Maintenance

Standard Maintenance Functions

Most security checks for maintenance functions are performed in the main menu. If the user does not have sufficient access rights, an error message is given.

Add

The user needs ADD access for the specified object type. For objects with subtypes, this subtype must also be entered so that a complete security check can be performed.

Copy

The user needs

- READ access for the object to be copied
- ADD access for the new object

For objects with subtypes, this subtype must also be entered so that a complete security check can be performed.

Modify

The user needs MODIFY access for the specified object.

Subtype

If the subtype can be modified, the system checks whether the user has sufficient access to the object with the new subtype. See function Rename.

Edit Owner

The user can only enter Y in the field Owner if he has at least READ access to the object type Owner.

Edit Child

The user can only enter Y in fields such as Program, for example, if he has at least READ access to the corresponding object type.

Parent object

If the parameter in parent can be specified, MODIFY access to the parent object is checked. If no permission has been granted, the field is read-only. A parent object cannot be modified.

Rename

The user needs MODIFY access to the specified object. An additional check is performed as to whether the renaming would lead to **increased** or **reduced** access.

- **Increased access** through Rename function

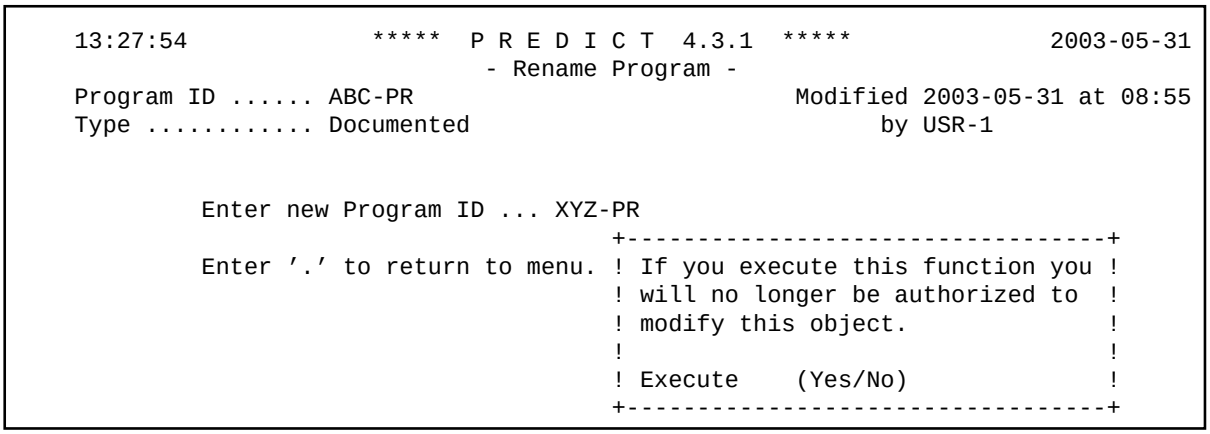
  If a Rename would lead to a user having increased access, the function cannot be executed and a message appears. The user must enter a new ID which would give him either the same or reduced access rights.

Example:
User USR-1 has no DELETE access to programs that start with ’ABC’, but he does have DELETE access to programs that start with ’X’.
Renaming the program ABC-PR to XYZ-PR would increase access rights of this user and is therefore not allowed.
The following message appears: "You are not authorized to execute this rename".

- **Reduced access** through Rename function

  If a Rename would lead to a user having reduced access rights, a window appears in which the user must confirm the loss of access rights. See example below.

  Example:
  User USR-1 has MODIFY access to programs that start with ’ABC’ but no MODIFY access to programs that start with ’X’.
  Renaming the program ABC-PR to XYZ-PR would restrict the user’s access rights. The user must confirm this loss of access explicitly.



Purge

The user needs DELETE access to the specified object.

Scratch

If objects of type database, system and program are deleted, subordinate objects are deleted, too. A security check is carried out for each object that is to be deleted additionally. If an object cannot be deleted, a message is given and this subordinate object is not deleted.

Master files

If a master file is deleted, all dependent userviews are deleted, too. Otherwise this would result in inconsistent data. If a userview cannot be deleted, the master file cannot be deleted either.

Edit Description

The user needs MODIFY access to the specified object.

Display

The user needs READ access for the specified object.

Link Children

User must have MODIFY access for the object whose link list is to be processed. No check is performed for the entries in the link list. If an object is READ-protected, the attributes are suppressed. The IDs of the linked objects are always displayed.

User must have at least READ access for the child object type. If this access has been granted, the entire link list can be processed.

With the Select function, the IDs of all objects are displayed. If an object is READ-protected, the attributes are not displayed and the object is marked with >>>protected<<<.

Edit Owner

The user needs READ access for the object type owner. For more information see function Link children, above.

Type-Specific Maintenance functions

This section is arranged alphabetically by object type.

Extract

The standard extract maintenance functions are subject to the normal maintenance checks. See Standard Maintenance Functions. The security checks for type-specific functions are described below.

Build / Extend and Extract

With this function, objects returned with a retrieval function can be put in an extract.

The following access is required.

- MODIFY access to the extract
- READ access to the object type specified.

When the function is started, the normal retrieval functions are carried out. This means that it is also possible that under certain circumstances protected objects are placed in the extract.

The same objects are placed in the extract irrespective of whether the user executed the List function.

Edit / Link Objects

This function is similar to the function Link children. However, since objects of different types can be linked to an extract, the security check of the function Link children is not applied. The following checks are performed instead:

- No READ access is required to object type of objects to be linked. If object type is protected, only the ID of the object is displayed; attributes are suppressed.
- The function Select is only available for object types for which the user has at least READ access.
- MODIFY access is required for the extract. The checks that are performed depend on the editor the user is working with:

Natural Editor

- When the object type is entered, the system checks that the user has READ access for this object type.
- With the List function, all objects of a type are displayed (as with Select function of the normal editors).

Software AG Editor

- No check is performed for linked object types.
- The user can enter any object in the editor. If he does not have READ access for an object, the ID of the object is displayed but attributes are suppressed.
- With the Select function, all objects of a type for which the user has permission are displayed for selection.

Export Extracts

The following access is required:

- READ access to the extract
- EXECUTE access to the Coordinator function Export (NSC object EXPORT).

Operate on Extracts

The following access is required:

- MODIFY access to the extract

The objects are added to or removed from the extract without additional checks.

File

Force Standard

With this function, only MODIFY access to the standard file is checked. No security checks on files affected by the rippling operation are carried out.

Note:
It would not make sense to check access of all objects. The user would need MODIFY access to all files affected by the rippling operation, even though, for example, he can access some of these files only via rippling and does not have access to them using normal maintenance functions.
MODIFY access to standard files should be granted sparingly!

Push Backward

The user needs MODIFY access to both files: to the first because it is modified, and to the second because new fields are inserted in the standard file with this function.

Other Edit Functions (Modify Adabas Attributes, Vista elements...)

The user needs MODIFY access to the specified file.

Owner

Edit Owner

If a new owner ID is specified, the user must have ADD access for this new object.
No security check is performed when an owner is deleted from the owner list of an object.

Program

Redocument Program

The user needs the following access to the program:

- ADD access if the program is added
- MODIFY access if an existing program is overwritten.

If a system is specified in which the programs are to be entered, the user must also have MODIFY access to this system.

Verification

With verifications it is the status and not the subtype that can be protected separately. When the command SAVE is entered in the Rule Editor, a security check is performed on the verification with the new status.

